AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method to facilitate locking an adversary out of a network application, comprising:

receiving at a server a request, including an authentication credential, to access the network application, wherein the authentication credential includes a user identifier associated with a user and a network address of a user device;

examining an audit log to determine if the user identifier has been locked out from the network address; and

if the user identifier has been locked out from the network address,

denying access to the network application;

otherwise, checking the authentication credential for validity, and

if the authentication credential is valid,

allowing access to the network application,

otherwise,

logging a failed attempt in the audit log, wherein the user identifier is locked out from the network address after a threshold number of failed attempts,

imposing a global lockout for the user identifier after a threshold number of network addresses are locked out for the user identifier, and

denying access to the network application;

whereby the adversary is prevented from accomplishing an attack by masquerading as the user.

2 (Canceled).

3. (Currently amended) The method of ~~claim 2~~claim 1, further comprising: removing ~~comprising removing~~ a lockout after a predetermined period of time.

4. (Currently amended) The method of ~~claim 2~~claim 1, further comprising: manually ~~comprising manually~~ removing a lockout by an administrator of the server.

5. (Original) The method of claim 1, wherein the authentication credential includes a user name and a password.

6. (Original) The method of claim 5, wherein checking the authentication credential for validity involves:

verifying that an administrator has authorized access to the network application for a combination of the user name and the password; and

determining if the request violates an access rule in a rule table.

7. (Original) The method of claim 6, wherein the access rule can specify:

an allowed time-of-day;

an allowed number of access attempts;

an allowed network address; and

an allowed network domain.

8. (Original) The method of claim 1, wherein the network address includes an Internet Protocol address.

9. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to facilitate locking an adversary out of a network application, comprising:

receiving at a server a request, including an authentication credential, to access the network application, wherein the authentication credential includes a user identifier associated with a user and a network address of a user device;

examining an audit log to determine if the user identifier has been locked out from the network address; and

if the user identifier has been locked out from the network address,

denying access to the network application;

otherwise, checking the authentication credential for validity, and

if the authentication credential is valid,

allowing access to the network application,

otherwise,

logging a failed attempt in the audit log, wherein the user identifier is locked out from the network address after a threshold number of failed attempts,

imposing a global lockout for the user identifier after a threshold number of network addresses are locked out for the user identifier, and

denying access to the network application;

whereby the adversary is prevented from accomplishing an attack by masquerading as the user.

10 (Canceled).

11. (Currently amended) The computer-readable storage medium of ~~claim 10~~claim 9, the method further comprising: removing ~~comprising removing~~ a lockout after a predetermined period of time.

12. (Currently amended) The computer-readable storage medium of ~~claim 10~~claim 9, the method further comprising: manually ~~comprising manually~~ removing a lockout by an administrator of the server.

13. (Original) The computer-readable storage medium of claim 9, wherein the authentication credential includes a user name and a password.

14. (Original) The computer-readable storage medium of claim 13, wherein checking the authentication credential for validity involves:

verifying that an administrator has authorized access to the network application for a combination of the user name and the password; and

determining if the request violates an access rule in a rule table.

15. (Original) The computer-readable storage medium of claim 14, wherein the access rule can specify:

an allowed time-of-day;

an allowed number of access attempts;

an allowed network address; and

an allowed network domain.

16. (Original) The computer-readable storage medium of claim 9, wherein the network address includes an Internet Protocol address.

17. (Currently amended) An apparatus to facilitate locking an adversary out of a network application, comprising:

a receiving mechanism that is configured to receive at a server a request, including an authentication credential, to access the network application, wherein the authentication credential includes a user identifier associated with a user and a network address of a user device;

an examining mechanism that is configured to examine an audit log to determine if the user identifier has been locked out from the network address; and

an access mechanism that is configured to deny access to the user identifier if the user identifier has been locked out from the network address;

a validation mechanism that is configured to check the authentication credential for validity, wherein the access mechanism is further configured to allow access if the authentication credential is valid; ~~and~~

a logging mechanism that is configured to log a failed attempt in the audit log, wherein the user identifier is locked out from the network address after a threshold number of failed attempts, and wherein the access mechanism is further configured to deny access to the user identifier after a failed access attempt;

a lockout mechanism that is configured to impose a global lockout for the user identifier after a threshold number of network addresses are locked out for the user identifier; and

whereby the adversary is prevented from accomplishing an attack by masquerading as the user.

18 (Canceled).

19. (Currently amended) The apparatus of ~~claim 18~~claim 17, further comprising: a ~~comprising a~~ lockout removing mechanism that is configured to remove a lockout after a predetermined period of time.

20. (Currently amended) The apparatus of ~~claim 18~~claim 17, further comprising: a ~~comprising a~~ lockout removing mechanism that is configured to allow an administrator of the server to manually remove a lockout.

21. (Original) The apparatus of claim 17, wherein the authentication credential includes a user name and a password.

22. (Original) The apparatus of claim 21, further comprising:

a verification mechanism that is configured to verify that an administrator has authorized access to the network application for a combination of the user name and the password; and

a violation determining mechanism that is configured to determine if the request violates an access rule in a rule table.

23. (Original) The apparatus of claim 22, wherein the access rule can specify:

an allowed time-of-day;

an allowed number of access attempts;

an allowed network address; and

an allowed network domain.

24. (Original) The apparatus of claim 17, wherein the network address includes an Internet Protocol address.